Quantisation Invariants for Transform Parameter Estimation in Coding Chains

Marco Visentini-Scarzanella[1] Marco Tagliasacchi[2] Pier Luigi Dragotti[1]

[1]Communications and Signal Processing Group
Imperial College London, London, United Kingdom.
[2] Dipartimento di Elettronica e Informazione
Politecnico di Milano, Milan, Italy.

Abstract

We examine the case of a signal going through a processing chain consisting of two transform coding stages, with the aim of recovering the unknown parameters of the first encoder. Through number theoretical considerations, we identify a lattice of quantisation invariant points, whose coordinates are not affected by the double quantisation and whose parameters are closely related to the unknown transform. The conditions for this lattice to exist are then discussed, and its uniqueness properties analysed. Finally, an algorithmic procedure to recover the invariants from a sparse set of points is shown together with numerical results.

1 Introduction

The effectiveness and computational simplicity of transform coding [1] has made it the *de facto* lossy compression standard for virtually all multimedia information that is shared on the web and stored in offline systems. This includes JPEG and JPEG2000 compression standards [2, 3] and H.26x compression algorithms [4].

Given the centrality of transform coding in widespread media objects, the information forensics community has turned its attention to the problem of uncovering the past history of objects that have been processed with coding chains, with applications including tampering detection, digital restoration and no-reference quality assessment. Some of the coding chains considered include single [5], double [6] or multiple [7] JPEG compression. Similar techniques have been also applied to video signals [8].

All of the works mentioned require knowledge of the specific coding standard employed. It is therefore important to develop methods to retrieve the transform parameters in a generic context, i.e. without any knowledge of the specific standard in use. Our work is similar in spirit to [9], where the authors present a method for recovering the transform parameters from a set of N observed points after single transform coding.

Many signals such as images however, are often compressed more than once. In this work, we focus on the case of a signal $\mathbf{x}$ with a more complex 'history' of two cascaded transform coding stages, consisting of the orthogonal transforms T_1, T_2 with uniform quantisation step sizes Δ_1 and Δ_2 respectively.

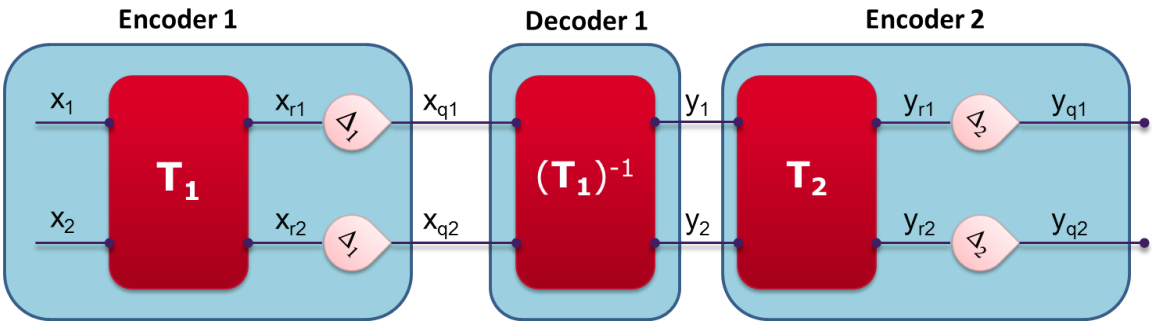


Figure 1: Double quantisation pipeline. The original signal $\mathbf{x}$ is encoded and decoded by an unknown orthogonal transform T_1 with uniform quantisation step Δ_1. The observed signal is re-encoded by a second transform T_2 (known) with quantisation step Δ_2

Following the pipeline shown in Figure 1, the signal $\mathbf{x}$ first undergoes a transform T_1, where T_1 is an orthogonal matrix with $\det(T_1) = 1$, yielding the rotated signal $\mathbf{x}_r$. This is then quantised into $\mathbf{x}_q$ by a uniform quantiser with step Δ_1, and decoded into $\mathbf{y}$ by inverting the initial transform T_1. The decoded signal $\mathbf{y}$ is encoded a second time by a system with known parameters T_2 and Δ_2, at which the quantised output $\mathbf{y}_q$ is observed.

Our contribution is to study the effect of the above coding chain on the signal structure in the case where only the parameters of the second coder are known. In particular, the aim of this work is to give an answer to the question of whether it is possible to uncover the individual coding operations in the context of a double encoding chain: starting from the final output $\mathbf{y}_q$, we aim to determine the conditions under which it is possible to navigate back up the signal's history to the first coding stage and determine the first encoder's exact transform parameters.

In the following sections, we analyse the requirements for the input signal and the two encoders in order to be able to recover the parameters of the first system. Whenever such requirements are satisfied, it is then possible to follow an algorithmic procedure to exactly recover the unknown parameters, as outlined in Section 4. Results are then presented in Section 5.

2 Effects of double quantisation

In this section, we examine the effect of the second quantisation on the spatial layout of the samples. Since the quantisation is performed independently along each dimension, the signal $\mathbf{x}_q$ observed after the first quantisation consists of samples from an upright square lattice. When considering the combined orthogonal transform $T_1^{-1}T_2$, the signal $\mathbf{y}_r$ will still consist of samples from a regular lattice rotated by the net transformation angle θ. At this stage in the processing chain, it would be still feasible to retrieve the transform parameters using, for example, the method in [9].

However, the second quantisation breaks the regularity of the original structure in

a nontrivial fashion, making it difficult to recover the parameters using basis reduction methods, especially if the second quantisation step is comparable in size to the first. Some examples of doubly quantised signals are shown in Figure 2(b), where $\Delta_2 = \frac{\Delta_1}{2}$.

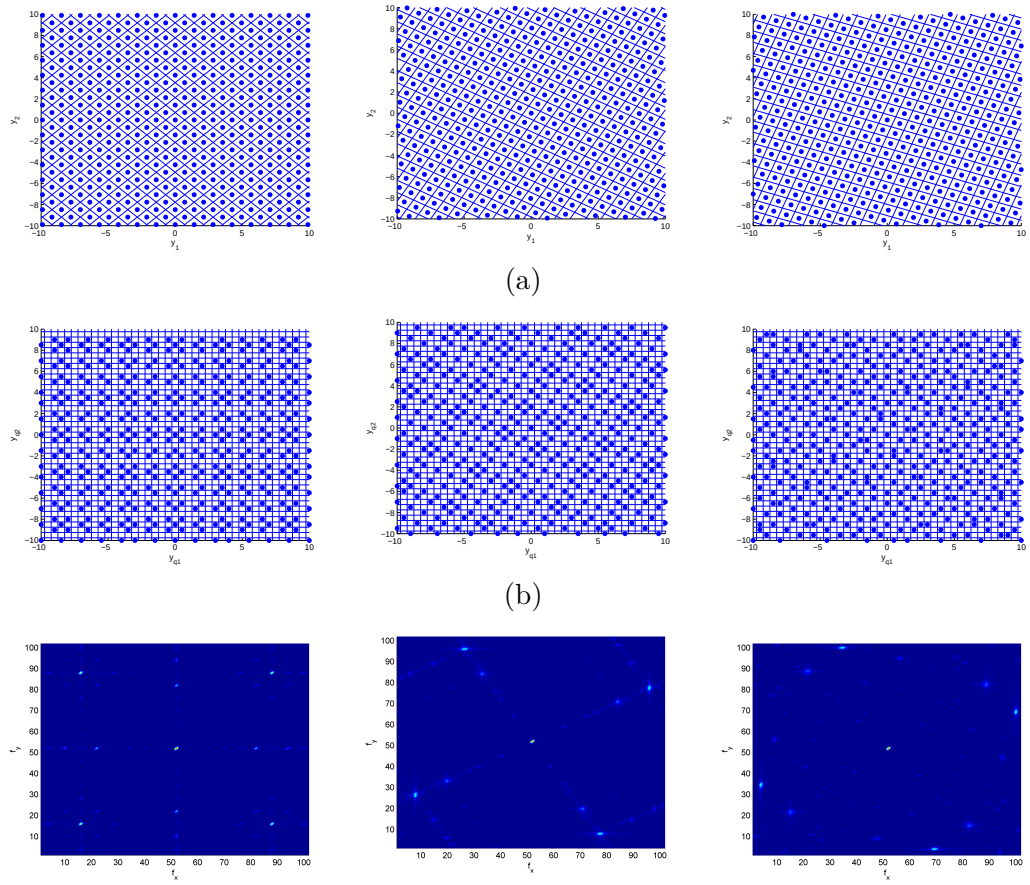


Figure 2: (a) The signal $\mathbf{y}_r$ after single quantisation and overall rotation by an angle θ is a regular lattice, here shown (from left to right) for $\theta = (\frac{\pi}{4}, \frac{\pi}{6}, \frac{\pi}{9})$. (b) The signal $\mathbf{y}_q$ after the second quantisation. (c) Fourier transform of (b).

Despite the radical effect on the signal's spatial layout, the spectrum of the original signal before the second quantisation is roughly preserved. Figure 2(c) shows the 2D-FT of the signals in (b), and the lattice structure of its peaks. It is worth noting how, despite the 'noise' introduced by the second quantisation making the signal's structure deviate from a lattice, the peaks in the Fourier domain still form a lattice whose orientation roughly reflects the net rotation angle θ. A 2D lattice rotated by an orthogonal matrix T maintains its structure during the Fourier transform, i.e.:

$$\begin{cases} \text{Ш}_2(Mt_1, Nt_1) = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} T\delta(t_1 - mM, t_2 - nN) \\ \mathcal{F}\left\{\text{Ш}_2(Mt_1, Nt_1)\right\} = \frac{1}{\det(T)} \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} T^{-1}\delta\left(f_1 - \frac{m}{M}, f_2 - \frac{n}{N}\right) \end{cases}. \quad (1)$$

However, while the Fourier peak orientation can provide information about θ despite the double quantisation, this still produces approximate results. The resolution is low, affecting the precision of the measurements especially for small angles, and most of the quantisation bins would have to be populated since for the transform relationship in (1) to be maintained a complete lattice as the input signal is required.

In the next section, we identify invariant points within doubly quantised signals that enable the exact recovery of the transform parameters, and we analyse the conditions for their existence.

3 Quantisation invariants

Quantisation is intimately related to modular arithmetic; the coordinates of the doubly quantised signal can be expressed in terms of the samples of the upright lattice indices $\mathbf{x}_q$ as:

$$\begin{bmatrix} y_{q1} \\ y_{q2} \end{bmatrix} = \Delta_2 \left\lfloor \frac{\Delta_1}{\Delta_2} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x_{q1} \\ x_{q2} \end{bmatrix} \right\rfloor, \quad (2)$$

where the rotated points $\mathbf{y}_r$ before the second quantiser correspond to:

$$\begin{bmatrix} y_{r1} \\ y_{r2} \end{bmatrix} = \Delta_1 \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x_{q1} \\ x_{q2} \end{bmatrix}. \quad (3)$$

After the second quantisation, the coordinates of every sample of $\mathbf{y}_q$ will be quantised to multiples of the second quantisation step Δ_2, i.e. by substituting Eq. (3) into (2):

$$\text{mod}\left(\Delta_2 \left\lfloor \frac{\mathbf{y}_{r(1,2)}}{\Delta_2} \right\rfloor, \Delta_2\right) = 0 \quad (4)$$

In order to characterise the periodicity of the points' structure in the (y_{q1}, y_{q2}) space, we are interested in the relationship between the rotated coordinates $\mathbf{y}_r = (y_{r1}, y_{r2})$ and their remainder $\mathbf{r} = (r_1, r_2)$ after quantisation with step Δ_2. If we consider a generic rotated point $\mathbf{y}_r$ and all its multiples with coordinates (ay_{r1}, by_{r2}), we can express the flooring effect introduced by quantisation as:

$$\begin{cases} \text{mod}\left(a\Delta_1(x_{q1}\cos\theta - x_{q2}\sin\theta), \Delta_2\right) &= r_1 \\ \text{mod}\left(b\Delta_1(x_{q1}\sin\theta + x_{q2}\cos\theta), \Delta_2\right) &= r_2 \end{cases}, (a, b) \in \mathbb{Z}. \quad (5)$$

We are interested in identifying sets of points that share the same quantisation remainder $\mathbf{r}$: if a relationship between the spacing and orientation of one such series

in (5) and the transform parameters can be established, it might be possible to obtain the unknown values directly from a subset of the samples after second quantisation. In particular we concentrate on the case where $(r_1, r_2) = \mathbf{0}$. In this case, the points $\mathbf{y}_q = \mathbf{y}_r$, are therefore invariant to the second quantisation. This means that if there are cases in which it is possible to have points that do not suffer from the flooring effect during quantisation, then these points will form a regular sequence as the solution of (5) whose characteristics depend on the unknown transform parameters.

Concerning the other cases where $(r_1, r_2) \neq \mathbf{0}$, we make use of basic number theoretical considerations. From the Linear Congruence theorem [10], we know that there are solutions to Eq. (5) if and only if the following relationships are satisfied:

$$\begin{cases} \gcd\left(\Delta_1(x_{q1}\cos\theta - x_{q2}\sin\theta), \Delta_2\right) | r_1, \\ \gcd\left(\Delta_1(x_{q1}\sin\theta + x_{q2}\cos\theta), \Delta_2\right) | r_2. \end{cases} \tag{6}$$

In Eq. (6) above, $\gcd(A, B)$ is the greatest common divisor operator between two terms, while $A|B$ indicates that term A divides term B. Given a sequence of samples consisting of a generic point with coordinates (x_{q1}, x_{q2}) rotated by an angle θ and all its multiples with coordinates (ay_{r1}, by_{r2}), the divisibility requirements in (6) are satisfied either if the rotated coordinates and the second quantisation step are coprime, or if the remainders are zero, i.e. the points in $\mathbf{y}_r$ are already exact multiples of the second quantisation step before the quantisation operation.

Guaranteeing that the rotated coordinates and the second quantisation step are coprime would be difficult, since there is no reason for the step size to be prime. Moreover, the fact that θ is a generic angle means that generally the pairs $(y_{r1}, \Delta_2), (y_{r2}, \Delta_2)$ would be incommensurable and the notion of greatest common divisor ceases to make sense.

Hence, we focus on the first case and characterise the set of points invariant to double quantisation. In the next section, we characterise the set of invariant points as a sublattice whose characteristics are related to the first transformation, and we analyse the conditions under which it is possible to recover the transformation history.

3.1 Pythagorean triples

In a practical system, it is unlikely for the steps to be irrational numbers. As a consequence, the condition in Eq. (6) implies that as a necessary condition for it to be true the points $\mathbf{y}_r$ must be rational numbers. Given that these points are the result of a rotation by an arbitrary angle θ, which will generally result in irrational coordinates, some constraint must be placed on the range of angles that can satisfy (6).

In general, the only angles that generate a rational result in a trigonometric function are those generated by Pythagorean triples [11]. Pythagorean triples are sets of three positive integers (a, b, c) representing the sides of a right-angle triangle satisfying

$$a^2 + b^2 = c^2, (a, b, c) \in \mathbb{N}^+, \tag{7}$$

where $\mathbb{N}^+$ is the set of positive integers. A generating formula for all primitive Pythagorean triples which results in all primitive right-angled triangles with integer sides is given by Euclid's formula [11]:

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2, \quad (u, v) \in \mathbb{N}^+. \tag{8}$$

From the definition, it is also possible to prove that there are infinitely many Pythagorean triples corresponding to as many different angles [11]. Additionally, in order to generate primitive Pythagorean triples, the integers u and v have to satisfy the following properties:

$$\begin{cases} \gcd(u, v) = 1 \\ (u - v) = 1 \mod 2 \\ u > v \end{cases}. \tag{9}$$

We also define $\frac{\Delta_1'}{\Delta_2'}$ to be the reduced form of the $\frac{\Delta_1}{\Delta_2}$ so that Δ_1', Δ_2' have no common factors. Having introduced the notions of Δ_1', Δ_2' and Pythagorean triples for rational trigonometric functions, we can now prove the following theorem about the lattice of invariants' structure.

Theorem 1. *Given a rotation angle θ representable by a Pythagorean triple generated by the integer tuple (u, v), there exists a lattice of invariants with step size $\mu = \Delta_2\Delta_1'\sqrt{u^2 + v^2}$ and orientation $\phi = \frac{\theta}{2}$.*

Proof. Given the generating equation for Pythagorean triples and substituting in place of the trigonometric functions, the doubly quantised points in Eq. (2) can be represented as:

$$\begin{cases} y_{q1} = \Delta_2 \left\lfloor \dfrac{\Delta_1'}{\Delta_2'} \left(\dfrac{u^2 - v^2}{u^2 + v^2} x_{q1} - \dfrac{2uv}{u^2 + v^2} x_{q2} \right) \right\rfloor, \\ y_{q2} = \Delta_2 \left\lfloor \dfrac{\Delta_1'}{\Delta_2'} \left(\dfrac{2uv}{u^2 + v^2} x_{q1} + \dfrac{u^2 - v^2}{u^2 + v^2} x_{q2} \right) \right\rfloor. \end{cases} \tag{10}$$

When substituting for (x_{q1}, x_{q2}) a point with coordinates $\alpha(u, -v)$, where u and v are the generators of the Pythagorean triple and α is an integer, Eq. (10) yields quantisation invariant points, i.e. points with integer coordinates before the second quantisation:

$$\begin{cases} y_{q1} = \Delta_2 \left\lfloor \dfrac{\Delta_1'}{\Delta_2'} \left(\dfrac{u^2 - v^2}{u^2 + v^2} \alpha u + \dfrac{2uv}{u^2 + v^2} \alpha v \right) \right\rfloor = \alpha' u \Delta_2 \Delta_1', \\ y_{q2} = \Delta_2 \left\lfloor \dfrac{\Delta_1'}{\Delta_2'} \left(\dfrac{2uv}{u^2 + v^2} \alpha u - \dfrac{u^2 - v^2}{u^2 + v^2} \alpha v \right) \right\rfloor = \alpha' v \Delta_2 \Delta_1', \end{cases} \tag{11}$$

where α is such that $\Delta_2' | \alpha$ and $\alpha' = \frac{\alpha}{\Delta_2'}$. Similarly, by substituting $\alpha(v, -u)$ one obtains $\alpha'(v, u)\Delta_2\Delta_1'$ after quantisation. Hence, all invariant points together create an oriented rectangular lattice Λ with orthogonal basis vectors $(\mathbf{v}_1, \mathbf{v}_2) = \Delta_2\Delta_1'([u, v], [v, u])$. The lattice step size μ stated in our theorem follows directly from the basis vectors.

Concerning the orientation angle $\phi = \tan^{-1}\frac{v}{u}$ of the lattice of invariants, this is related to the angle θ as initially stated in our theorem, since:

$$\tan^2(\phi) = \frac{v^2}{u^2} = \frac{1 - \frac{u^2-v^2}{u^2+v^2}}{1 + \frac{u^2-v^2}{u^2+v^2}} = \frac{1-\cos(\theta)}{1+\cos(\theta)} \Rightarrow \phi = \frac{\theta}{2}, \tag{12}$$

which concludes our proof. □

Summarising, in this section we have demonstrated that if the rotation angle can be generated by a Pythagorean triple, the doubly quantised points will contain an invariant lattice whose orientation and step size can be used to recover exactly the original transform. What remains to be proven is that the invariant lattice found in (11) is not a sublattice of another invariant lattice as well as the only possible invariant lattice that can be found. This will be shown in the next section.

3.2 Uniqueness of invariant lattices

We can test the existence of alternative invariant points by assuming that instead of a point with coordinates proportional to the Pythagorean triple generators as found in Eq. (11), we have a generic point $\mathbf{x}_q = (x_{q1}, x_{q2})$. In this case, the point will be invariant to quantisation if the denominator in Eq. (10) is cancelled out, i.e.:

$$\begin{cases} (u^2-v^2)x_{q1} - (2uv)x_{q2} = t_1(u^2+v^2) \\ (2uv)x_{q1} + (u^2-v^2)x_{q2} = t_2(u^2+v^2) \end{cases}, (t_1, t_2) \in \mathbb{Z}. \tag{13}$$

The system above implies that the left hand sides must have some common factors (t_1, t_2) that can be factored out. But since $\gcd(u, v) = 1$ by the properties of Pythagorean triples generators in (9), then the common factors must be represented by the coordinates (x_{q1}, x_{q2}). Therefore, there is a limited number of possibilities of what these common factors can be. In particular, x_{q1} can be of any form from the set $\{2, \alpha_1 x_{q2}, \alpha_1 u, \alpha_1 v\}$, where α_1 is an integer. Similarly x_{q2} can be of any form from the set $\{2, \alpha_2 x_{q2}, \alpha_2 u, \alpha_2 v\}, \alpha_2 \in \mathbb{Z}$.

If we assume that $x_{q1} = \alpha_1 x_{q2}$, then $t_1 = t_2 = x_{q2}$ and by simplifying and rearranging the two equations in the system, we have:

$$\begin{cases} \alpha_1(u^2-v^2) - 2uv = u^2+v^2, \\ \alpha_1 u = v. \end{cases} \tag{14}$$

Taking under consideration the second equation in the system, we have that $\alpha u = v$. However, from the properties of (u, v) in (9), u and v do not have any common factors, hence we have a contradiction and $x_{q1} \neq \alpha_1 x_{q2}$. By a similar argument, $x_{q2} \neq \alpha_1 x_{q1}$. Therefore, $\gcd(x_{q1}, x_{q2}) = 1$.

Considering the possibility that $x_{q1} = 2$, we notice that in order to have a common factor in both equations in the system then either $x_{q2} = 2$, which would not be possible since $\gcd(x_{q1}, x_{q2}) = 1$, or $x_{q2} \in \{\alpha_2 u, \alpha_2 v\}$. But if this were the case, then $x_{q1} = 2$ is just a special instance of $x_{q1} = \alpha_1 u$, and $x_{q2} = \alpha_2 v$. Therefore, the only possible solutions are that $(x_{q1}, x_{q2}) \in \{\alpha_2 u, \alpha_2 v\}$, with the additional constraint that

if $x_{q1} = \alpha_1 u$ then $x_{q2} = \alpha_2 v$ and vice versa. We now proceed to verify that the solution found in (11) represents the fundamental lattice and not a sublattice of the real solution. Substituting $(\alpha_1 u, \alpha_2 v)$ for (x_{q1}, x_{q2}) in (13) and factorising:

$$\begin{cases} u(\alpha_1 u^2 - \alpha_1 v^2 - 2\alpha_2 v^2) = t_1(u^2 + v^2), \\ v(\alpha_2 u^2 - \alpha_2 v^2 + 2\alpha_1 u^2) = t_2(u^2 + v^2). \end{cases} \tag{15}$$

Since (u, v) are the only elements that can be factored out, it follows that $t_1 = u$ and $t_2 = v$ respectively. Combining the two equations and simplifying we have a relationship linking α_1 and α_2:

$$\begin{aligned} &- \alpha_1(u^2 + v^2) = \alpha_2(u^2 + v^2) \\ &\Rightarrow \alpha_1 = -\alpha_2 \end{aligned} \tag{16}$$

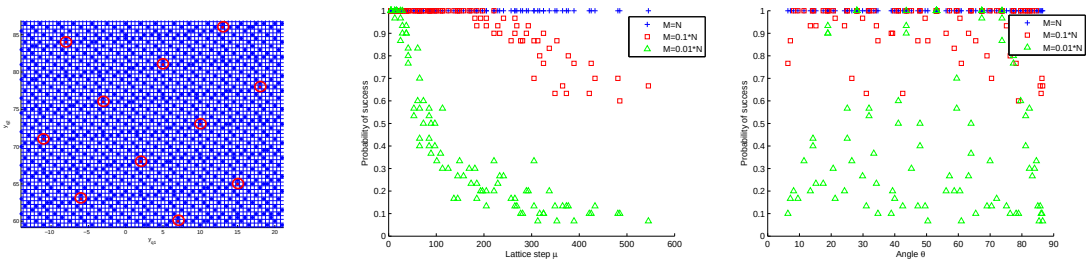
Since α_1 and α_2 are integers by definition, it follows that the lattice found in (11) is the fundamental lattice, where $(\alpha_1, \alpha_2) \in \{1, -1\}$. Given the uniqueness property of the lattice of invariants, we present a simple algorithmic procedure to test the observed samples and check automatically their conformity to the lattice. This procedure is described in the next section.

4 Algorithmic solutions

Based on the characteristics of the lattice of invariants Λ and its uniqueness highlighted in the previous section, we devise some simple criteria that can be used to test whether one of the observed samples in $\mathbf{y}_q$ belongs to Λ. While in this section we assume knowledge of the first quantisation step size Δ_1, it is possible to retrieve it with existing methods such as [12].

We start with a candidate set containing all observed points. Since all invariant points lie on Λ, it follows that they lie on concentric circumferences centred at the origin and with radii multiples of $\Delta_2\Delta_1'$. Therefore, it is possible to remove from the set of invariant candidates all points whose squared norm is not divisible by $(\Delta_2\Delta_1')^2$. For uniformly distributed points, this criterion removes all but $N(\frac{\Delta_2}{\Delta_1})^2$ points, where N is the number of points observed.

All remaining points have a squared norm that is an integer multiple of $(\Delta_2\Delta_1')^2$. Based on the invariant lattice properties, it follows that the squared norm of any point belonging to Λ can be expressed as $(\Delta_2\Delta_1')^2(m^2u^2 + n^2v^2), (m, n) \in \mathbb{Z}$. Therefore, given the squared norm $(\frac{||\mathbf{y}_q||}{\Delta_2\Delta_1'})^2$ of a point divided by $(\Delta_2\Delta_1')^2$ to the candidate set, it is possible to algorithmically compute its integer partition into a sum of $m^2 + n^2$ squares of only two distinct terms. If such decomposition exists, and the two terms being summed together are the generators of a Pythagorean triple according to the properties outlined in (9), then the transform parameter θ can be computed automatically from ϕ. Finding a point belonging to Λ concludes our iteration, as from it alone it is possible to generate the rest of the lattice, recover the transform parameter and check against



(a) (b) (c)

Figure 3: (a) An example of a recovered invariant lattice (red). Probability of success of the algorithm against: (b) invariant lattice spacing μ and (c) transform angle θ for various sparsity levels of the input signal.

the other observed samples. As an example, consider three of the integer partitions of 281 into a sum of squares:

$$281 = \left\{2 \cdot 10^2 + 1 \cdot 7^2 + 2 \cdot 4^2, 2 \cdot 10^2 + 1 \cdot 9^2, \cdots, 4 \cdot 8^2 + 1 \cdot 5^2\right\}. \tag{17}$$

Considering the first decomposition, it can be automatically ruled out since it is the sum of three distinct squares, not two. In the second decomposition, the multiplicity criterion is not satisfied, since 2 is not the square of an integer, hence $m^2 \neq 2$. The third decomposition satisfies all the aforementioned requirements.

We now show how these simple criteria are sufficient to reliably find the transform parameter given a θ generated by a Pythagorean triple even with very sparse inputs.

5 Results

Figure 3 shows the probability of success of the algorithm for various sparsity levels of the input signal: given an input signal initially quantised into N^2 samples ($N = 100$ in our tests) $\mathbf{x}_q = [0 \cdots N] \times [0 \cdots N]$, we consider M randomly selected samples, where $M = \beta N$, and $\beta \in \{1, 0.1, 0.01\}$. The experiments have been run with fixed quatisation steps $(\Delta_1, \Delta_2) = (1, \frac{1}{2})$ and considering the first 100 randomly generated Pythagorean triples representing angles $\theta \in (0, \frac{\pi}{2})$. For every angle θ considered, we averaged the probability of success over 30 runs of the algorithm.

From Figure 3 (a), the main parameter affecting the algorithm is the relative size of the invariant lattice step μ, which determines the density of the lattice of invariants, compared to the input domain size N. This is related to the Pythagorean triple generators u and v as well as the steps Δ_1 and Δ_2. The algorithm is guaranteed to find the correct transform parameter if a single invariant is left in the input, and Figure 3 (b) shows that even for larger values of μ the probability of finding the correct parameter stays above 60% in our experiments even when only 10% of the input samples are considered.

It would be desirable to identify a relationship between the probability of success and the angle θ. However, the relationship between the angle and the lattice step is

highly unpredictable as it depends not on the angle but on the Pythagorean triple generators u and v, making it difficult to qualitatively estimate the density of invariants given an angle. This is evidenced when comparing the trend of the results in Figure 3 (a) and (b), and formalised in the lattice properties stated in Theorem 1.

6 Conclusions

In this paper, we studied the conditions under which it is possible to exactly recover the coder's parameters after a double quantisation chain. Using number theoretical notions, we have shown how for an infinite set of angles generated by Pythagorean triples, there exists a unique lattice of invariant points whose characteristics are directly linked to the transform parameter. We have also provided some simple criteria to algorithmically recover the parameter given a very sparse set of observations.

Acknowledgements: This work was supported by the REWIND Project funded by the Future and Emerging Technologies (FET) programme within the FP7 Programme of the European Commission, under FET-Open grant number: 268478.

References

[1] V. K. Goyal, "Theoretical foundations of transform coding," *IEEE Signal Processing Magazine*, vol. 18, no. 5, pp. 9–21, September 2001.

[2] G.K. Wallace, "The JPEG still picture compression standard," *IEEE Transactions on Consumer Electronics*, vol. 38, no. 1, pp. xviii–xxxiv, feb 1992.

[3] D.T. Lee, "JPEG 2000: Retrospective and new developments," *Proceedings of the IEEE*, vol. 93, no. 1, pp. 32–41, jan 2005.

[4] G.J. Sullivan and T. Wiegand, "Video compression - from concepts to the H.264/AVC standard," *Proceedings of the IEEE*, vol. 93, no. 1, pp. 18–31, jan 2005.

[5] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," *IEEE Transactions on Image Processing*, vol. 12, no. 2, pp. 230–235, 2003.

[6] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1003–1017, June 2012.

[7] S. Milani, M. Tagliasacchi, and S. Tubaro, "Discriminating multiple jpeg compression using first digit features," in *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, march 2012, pp. 2253–2256.

[8] S. Milani, M. Fontani, P. Bestagini, M. Barni, A. Piva, M. Tagliasacchi, and S. Tubaro, "An overview on video forensics," *APSIPA Transactions on Signal and Information Processing*, vol. 1, pp. 1–18, 2012.

[9] M. Tagliasacchi, M. Visentini Scarzanella, P. L. Dragotti, and S. Tubaro, "Transform coder identification based on quantization footprints and lattice theory," *ArXiv e-prints*, November 2012.

[10] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, OUP Oxford, 2008.

[11] J. H. Silverman, *A Friendly Introduction to Number Theory*, Pearson Education, 2012.

[12] S.D. Casey and B.M. Sadler, "Modifications of the euclidean algorithm for isolating periodicities from a sparse set of noisy measurements," *IEEE Transactions on Signal Processing*, vol. 44, no. 9, pp. 2260–2272, sep 1996.